Chapter 48
Securing Biometrics Using Watermarking

Punam Bedi
University of Delhi, India

Roli Bansal
University of Delhi, India

Priti Sehgal
University of Delhi, India

ABSTRACT

This chapter focuses on the role of watermarking techniques in biometric systems. Biometric systems are automated systems of verifying or recognizing the identity of a living person based on a physiological or behavioral characteristic. While biometric-based techniques have inherent advantages over other authentication techniques, ensuring the security and integrity of data is a major concern. Data hiding techniques are thus used in biometric systems for securing biometric data itself. Amongst all the biometric techniques, fingerprint-based identification is the oldest and the most well established method used in numerous applications because fingerprints are unique and they remain unchanged during the human life span. However, fingerprint images should be watermarked without affecting their quality and their minutia matching ability. Moreover, if the watermark embedded in the fingerprint image is the face image of the same individual, the watermarking scheme will have two levels of security such that it will not only protect the cover fingerprint but also provides a more secure system of personal recognition and authentication at the receiver's end. This work finds application in a number of security implementations based on multimodal biometric authentication. Computationally intelligent techniques can be employed to develop efficient watermarking algorithms in terms of watermarked image quality and distortion tolerance ability.

DOI: 10.4018/978-1-4666-8789-9.ch048

INTRODUCTION

Biometric technologies refer to different automated methods for verifying or recognizing the identity of an individual based on one or more of his physical and behavioral characteristics. The word automated refers to methods that are carried out by a machine, generally a computer. Physical characteristics in biometrics typically include fingerprints, eye retinas and irises, facial patterns and hand measurements. Behavioral characteristics typically include signatures, gait, or typing patterns. The primary biometric disciplines include: fingerprints (optical, silicon, ultrasound, touch less), facial recognition (optical and thermal), voice recognition, iris recognition, retina-scan, hand geometry, signature-scan, keystroke-scan, palm-scan (forensic use only) etc. There are some biometric disciplines with reduced commercial viability and some are in exploratory stages such as: DNA, ear shape, odour (human scent), vein-scan (in back of hand or beneath palm), finger geometry (shape and structure of finger or fingers), nail bed identification (ridges in fingernails), gait recognition (manner of walking) etc. The selection of a particular biometric depends on the application where it is going to be used. Jain et al identified seven such factors which can be used for assessing the suitability of any characteristic for use in biometric authentication. They also said that no single biometric will meet all the requirements of every application. (Jain, Bolle, & Pankanti, 1999). These factors include:

1. **Universality:** Every person using the system should possess the selected biometric trait.
2. **Uniqueness:** The biometric trait under study should be different for different people in the population so as to correctly distinguish them from one another.
3. **Permanence:** The trait should be invariant over time with respect to the specific matching algorithm.
4. **Collectability:** The trait should be collectable i.e., the acquisition or measurement of the trait should be practically feasible.
5. **Performance:** The identification accuracy using the selected biometric trait should be acceptable.
6. **Acceptability:** The individuals in the relevant population must be willing to have their biometric trait captured and assessed.
7. **Circumvention:** The trait should not be imitated using an artifact or substitute so as to fool the system using fraudulent techniques.

A Biometric system operates in the following two modes (Jain et al, 2008): *Identification* mode, where the system performs a one-to-many comparison against a biometric database in an attempt to establish the identity of an unknown person. *Verification* mode, where the system performs a one-to-one comparison against a specific template stored in a biometric database to determine if the person under scrutiny is authorized one.

SECURITY AND AUTHENTICATION OF BIOMETRIC DATA

While biometric-based techniques have inherent advantages over other authentication techniques, ensuring the security and integrity of data is a major concern. The tremendous growth in distribution of digital data through the Internet has raised serious authentication issues. Moreover, if biometric datasets fall into criminal hands, they could be used to impersonate individuals, and thereby allow criminals to evade safeguards intended to identify and apprehend them. They can also be used to falsely incriminate an innocent individual in a physical crime.

For a biometrics based verification system to work properly, the verifier system must ensure the legitimate origin of the biometric data at the time of enrollment. In on-line transaction processing